robocheckin.com

RoboCheckIn User Guide

Complete documentation for all features and menus

Beta — All features free

Table of Contents

1. What is RoboCheckIn?

Uptime monitoring & infrastructure health platform

RoboCheckIn is an open-beta SaaS platform that monitors the availability, performance, and security of your web services, APIs, domains, and LLM endpoints. It alerts your team the moment something goes wrong — before your users notice.

Core capabilities

- HTTP/HTTPS uptime monitoring with keyword and JSON assertions
- SSL certificate expiry tracking and alerts
- DNS resolution monitoring
- TCP port availability checks
- ICMP Ping / latency measurement
- Heartbeat / Cron job monitoring (dead-man's switch)
- LLM data-leak and prompt-injection testing
- Public status pages for your customers
- Incident management with timeline and comments
- Alert rules with escalation to Slack, Discord, Telegram, Email

> Beta: All Pro-tier features are free for everyone. No credit card required. Monitors check every 30 seconds.

2. Quick Check — Instant Test

No account needed · results in seconds

The Quick Check tool on the homepage lets you run a one-off check on any target without creating an account. Results are displayed immediately in the browser and are not stored.

Check types

Type	What it checks	Example input
HTTP	HTTP status code, response time, availability	https://example.com
SSL	Certificate validity, issuer, days until expiry	example.com

DNS	DNS resolution, returned records (A, CNAME…)	example.com
TCP	TCP port open/closed, connection time	example.com:443
Ping	ICMP reachability, packet loss %, avg RTT (ms)	8.8.8.8

How to use

- Select check type from the tab bar (HTTP / SSL / DNS / TCP / Ping)
- Enter the target URL, domain, or IP address
- Click Check — results appear within 3–5 seconds
- Results show: status, response time, and type-specific detail

3. Dashboard

Real-time overview of your entire infrastructure

The Dashboard is your mission-control screen. It loads on login and refreshes automatically every 30 seconds.

Summary cards

- Total monitors and counts per status
- Open incidents count
- Monitors needing attention highlighted in red

Monitor list

- Status badge: UP / DOWN / DEGRADED
- Last response time (ms)
- Next check countdown

Status meanings

UP — All checks passing within normal thresholds.

DEGRADED — Endpoint responding but slower than expected or with warnings.

DOWN — Check failed. Alerts will be triggered per your rules.

4. Monitors

Automated, recurring checks for all your endpoints

Monitors run continuously at your chosen interval. Each monitor stores the full history of checks, allowing you to see uptime trends and response-time graphs over time.

Creating a monitor

- Go to Monitors ’ New Monitor
- Choose the monitor type (see table below)
- Fill in the required fields (URL, interval, thresholds)
- Optionally add HTTP headers, keywords, or JSON path assertions
- Click Create — monitoring begins immediately

Monitor types

Type	Description & key fields

HTTP / HTTPS	Sends an HTTP request and checks the response code. Optionally verify a keyword in the body or match a JSON path value. Set expected status codes and response-time thresholds.
SSL Certificate	Checks TLS certificate validity and days remaining. Set alert threshold (e.g. alert when < 30 days left). Also verifies issuer chain.
DNS	Resolves the domain and verifies the returned records match expected values. Supports A, AAAA, CNAME, MX, TXT record types.
TCP Port	Attempts a TCP connection to host:port. Reports open/closed and connection time. Useful for databases, SMTP, and custom services.
Ping (ICMP)	Sends ICMP echo requests and reports packet loss % and round-trip time. Requires the host to allow ICMP.
Heartbeat / Cron	Expects a periodic HTTP ping from your service. If no ping arrives within the interval, the monitor goes DOWN. Ideal for cron jobs and background workers.

Monitor detail page

Click any monitor name to open its detail page. Here you can see:

- Live status and last check result
- Response time chart (7 days by default)
- Uptime % over 24h / 7d / 30d / 90d
- Full check history log with timestamps and response codes
- Edit and delete options

Heartbeat / Cron setup

After creating a Heartbeat monitor, copy the unique ping URL shown on the detail page. Add a cURL call to your cron job or script:

```
curl -s https://robocheckin.com/api/v1/hb/<your-token>
```

Call this URL at the end of each successful job run. If the URL is not called within the expected interval, an alert is fired.

5. Incidents

Track, communicate, and resolve outages

Incidents represent real service disruptions. They can be created automatically by alert rules or manually by your team. Each incident has a timeline of events, severity, and status.

Incident lifecycle

Status	Meaning
Open	Incident is active. Team is investigating or working on a fix.
Monitoring	Fix applied, watching to confirm recovery.
Resolved	Service restored. Incident closed.

Creating an incident manually

- Go to Incidents ' fill in the Create Incident form
- Title: short description of what is failing
- Summary: detailed explanation of the impact
- Severity: Minor / Major / Critical
- Click Create — incident appears in the timeline immediately

Managing incidents

- Add comments to the timeline to communicate updates to stakeholders
- Click Resolve when the issue is fixed
- Resolved incidents are kept in history for post-mortem review
- Incidents auto-refresh every 5 seconds when the page is visible

Severity levels

- Minor — limited impact, workaround available
- Major — significant disruption, no workaround
- Critical — full outage or data loss risk

6. Alert Rules

Define when and how your team is notified

Alert Rules determine what events trigger notifications and incidents. You can create rules that target all monitors or a specific monitor, with fine-grained control over triggers, severity, and deduplication.

Creating an alert rule

- Go to Alert Rules ’ fill in the form
- Name: descriptive label (e.g. 'API Down ’ PagerDuty')
- Monitor: leave blank to apply to all monitors, or select one
- Triggers: select one or more events that fire the rule
- Severity: Minor / Major / Critical
- Dedupe window: suppress duplicate alerts for N minutes
- Auto-create incident: automatically open an incident when fired

Available triggers

Trigger	When it fires
down	Monitor transitions from UP/DEGRADED to DOWN
degraded	Monitor becomes slower than threshold (DEGRADED status)
ssl_expiry	SSL certificate is within expiry threshold window
heartbeat_missed	Heartbeat monitor didn't receive a ping in time
recovery	Monitor recovers from DOWN or DEGRADED back to UP

Notification channels

Configure channels in Settings ’ Notifications. Supported integrations:

- Slack — webhook URL, messages sent to chosen channel
- Discord — webhook URL, rich embed messages
- Telegram — Bot token + Chat ID
- Email — SMTP or API-based delivery

> Tip: Create a 'recovery' alert rule alongside your 'down' rule so your team is automatically notified when service is restored.

7. Status Pages

Public-facing uptime pages for your customers

Status Pages give your users real-time visibility into your service health, without requiring any login. Share the URL with customers, embed it in your documentation, or link from your support portal.

Creating a status page

- Go to Status Pages ’ fill in the creation form
- Name: visible title of the page (e.g. 'Customer Portal Status')
- Slug: URL-friendly identifier (auto-generated from name)
- Description: what systems this page covers
- Monitors: select which monitors appear on the page
- Public: toggle to make the page accessible without login
- Maintenance message: optional banner shown at the top of the page

Accessing the status page

Public status pages are available at: **robocheckin.com/status/your-slug**

- No login required for public pages
- Shows real-time status for each selected monitor
- Displays response time and uptime percentage
- Maintenance banner is shown when maintenance message is set

Managing status pages

- Multiple status pages can be created (e.g. one per product)
- Delete a page using the trash icon in the list
- Update monitors by deleting and recreating the page

> Pro tip: Create separate status pages for different customer segments — internal teams might see more monitors than public-facing pages.

8. LLM Leak Tests

Test your AI endpoints for data leaks and prompt injection

LLM Leak Tests help you verify that your AI-powered endpoints are not accidentally returning sensitive data embedded in prompts, system messages, or context. This is critical for any product that uses LLMs (GPT, Claude, Gemini, etc.) in production.

How it works

- You create Canary Secrets — fake but realistic secrets (API keys, passwords, etc.)
- These canaries are injected into prompts sent to your LLM endpoint
- The response is scanned to see if the canary was leaked in the output
- If found, a finding is recorded with severity and the leaked snippet

Tab: Canaries

Canary secrets are auto-generated fake credentials. You choose:

- Name: descriptive label (e.g. 'Prod API Key Canary')
- Category: API Key / Password / Token / PII / Credit Card

The actual canary value is auto-generated and stored encrypted. You never see it.

Tab: Suites

A Test Suite defines which endpoint to test and how:

- Target URL: your LLM API endpoint (e.g. https://api.openai.com/v1/chat/completions)
- Method: POST or GET
- Prompt template: the prompt with {{canary}} placeholder

The placeholder {{canary}} is replaced with the actual canary value at test time.

Tab: Runs

- Click Run on a suite to start a test
- Each run tests all canary secrets against the suite endpoint
- Results show: total checks, leaked count, findings with severity
- Findings include: severity (critical/high/medium/low), source type, leaked snippet

> If canary secrets appear in LLM responses, your system prompt may be exposed. Review your prompt injection controls and context window construction.

9. Settings & Notifications

Configure integrations and workspace preferences

The Settings page lets you configure notification channels, manage API tokens, and control workspace-level preferences.

Notification channels

Channel	Setup steps
Slack	Create an Incoming Webhook in your Slack workspace. Paste the webhook URL in Settings. Test with the Send Test button.
Discord	Right-click a channel ’ Edit Channel ’ Integrations ’ Webhooks ’ New Webhook. Copy URL, paste in Settings.
Telegram	Create a bot via @BotFather. Copy the Bot Token. Start a chat with the bot and get the Chat ID via /getUpdates. Enter both in Settings.
Email	Enter recipient email address(es). Alerts are sent from noreply@robocheckin.com. Check spam folder on first setup.

10. Guest Mode vs Registered Account

Guest Mode

- No account required
- All features accessible
- Data stored in browser session (24 hours)
- Quick Check: instant, no storage
- Data lost when browser session ends

Registered Account

- Free signup, no credit card
- Data stored permanently
- Multi-workspace support
- 90-day data retention
- API token access

11. API Access

Automate and integrate via REST API

RoboCheckIn provides a REST API for programmatic access to all resources. Generate an API token in Settings ’ API Tokens.

Authentication

```
Authorization: Bearer <your-api-token>
```

Base URL

```
https://robocheckin.com/api/v1
```

Key endpoints

- GET /workspaces — list your workspaces
- GET /workspaces/{id}/monitors — list monitors
- POST /workspaces/{id}/monitors — create monitor
- GET /workspaces/{id}/incidents — list incidents
- POST /workspaces/{id}/incidents — create incident
- GET /workspaces/{id}/alert-rules — list alert rules
- GET /v1/guest/check — instant check (no auth)

12. Frequently Asked Questions

How often do monitors check?

During beta: every 30 seconds. Post-beta plans will offer 15-second intervals on Team plan.

How long is data retained?

90 days for registered accounts. Guest data lasts for the browser session (up to 24 hours).

Is there a monitor limit?

No limit during beta. Post-beta Free plan will include 10 monitors.

How do I get support?

Email: techsyncanalyticallc@gmail.com — or use the contact link on the pricing page.